



1990.62597

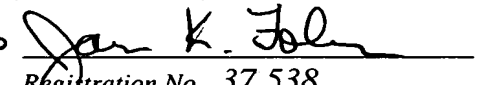
PATENT

419

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Patent Application )  
Applicant: Utsumi et al. )  
Serial No.: 09/159,833 )  
Filed: September 24, 1998 )  
For: STORING APPARATUS AND )  
AND PASSWORD CONTROL )  
METHOD )  
Art Unit: 2131 )  
Examiner: Jackson, Jenise E. )

*I hereby certify that this paper is being deposited with the United States Postal Service as FIRST-CLASS mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this date.*

8/21/2003   
Date Registration No. 37,538  
F-CLASS.WCM  
Appr. February 20, 1998 Attorney for Applicant

**RECEIVED**

AUG 28 2003

Technology Center 2100

SUBMISSION OF VERIFIED TRANSLATION OF JP 62-9471

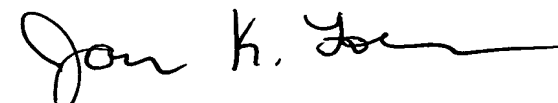
Commissioner for Patents  
P.O. Box 1450  
Alexandria, VA 22313-1450

Dear Sir:

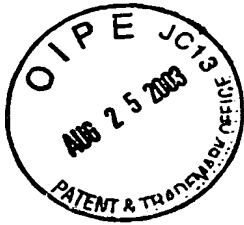
Attached hereto is a verified translation of JP 62-9471, including a Certificate signed by the translator.

Respectfully submitted,

GREER, BURNS & CRAIN, LTD.

By   
James K. Folker  
Registration No. 37,538

August 21, 2003  
300 South Wacker Drive  
Suite 2500  
Chicago, Illinois 60606  
Telephone: 312.360.0080  
Facsimile: 312.360.9315



## CIRTIIFICATE

RECEIVED

AUG 28 2003

Technology Center 2100

I, Hideaki KOGURE of 8th floor, Shimizu Building, 25-47, Nishi-Shinbashi 3- chome, Minatoku, Tokyo 105-0003, Japan, hereby certify that I am the translator of JP62-9471(A), and certify that the following is a true and correct translation to the best of my knowledge and belief.

BY: Hideaki Kogure  
Hideaki KOGURE

Dated this 8 day of August 2003



Japanese Unexamined Patent Application Publication

No. 62-9471

**RECEIVED**

AUG 28 2003

SPECIFICATION

Technology Center 2100

5

1. Title of the Invention

CONFIRMING DEVICE FOR PASSWORD INFORMATION OF  
INTEGRATED CIRCUIT CARD

10 2. Claims

A confirming device for password information of an  
integrated circuit card which previously stores password  
information of an IC card comprising means for entering a  
signal intrinsic to an IC card to be connected and  
15 recognizing the kind of said card; means for comparing and  
collating said password information previously stored  
corresponding to the IC card specified by said card  
recognizing means and password information stored in said  
specific IC card itself; and means for outputting the  
20 password information under said collating means upon  
determining consistency between said two kinds of password  
information.

3. Detailed description of the Invention

25 [Technical Field of the Invention]

The present invention relates to a confirming device  
for password information of an integrated circuit card

which outputs, as required, password information of an IC card used as a cash card or a credit card issued by a financial institution such as a bank.

## 5 [Related Art and Problems]

Recent and present years are called the cashless era in which commercial goods can be purchased without using cash by using a card issued by a credit card issuer company or the like. Such cards in common use conventionally include  
10 plastic cards, embossed cards, and magnetic stripe cards. However, these cards permit easy forgery in structure, posing a problem of fraudulent use. For the purpose of solving this problem, there has been developed an information card in which an IC circuit storing a password  
15 number and other information is incorporated so that the password number is not easily read out from outside, known as an IC card. The IC card is hard to be forged and excellent in security, advantageous in that it can store many pieces of information. Particularly, because of the  
20 possibility for the owner to directly set and enter a personal password number by himself/herself, the password number is never known by an other (for example, by a bank clerk), leading to a very high safety.

However, when using the above-mentioned IC card in  
25 practice, a card owner himself/herself often forgets his/her password number. In this IC card of which the password number is never known by any other at all, a

problem is that the only way is to abolish the card unless the card owner himself/herself remembers the password number.

5 [Object of the Invention]

The present invention was developed in view of the above-mentioned problems and has an object to provide a confirming device for password information of an integrated circuit card which, for example, even when the card owner  
10 himself/herself forgets his/her password number, permits reconfirmation of the password number information stored in the card.

[Gist of the Invention]

15 More specifically, the confirming device for password information of an integrated circuit card has a configuration based on a process comprising the steps of writing password information into an IC card and simultaneously previously storing the password information  
20 in this device; recognizing the kind of card from an intrinsic signal from the IC card connected later, and outputting and confirming the above-mentioned previously stored password information in response to this recognized specific IC card.

25

[Embodiments]

An embodiment of the present invention will now be

described with reference to the drawings.

Fig. 1 illustrates an exterior view configuration of the confirming device for password information of an integrated circuit card. A keyboard 2, a display part 3 and a printer part 4 are provided on the main body upper surface of a printer-calculator 4 with a terminal of this device. The above-mentioned keyboard 2 has calculating keys such as ten-keys and function keys as well as an IPIN key 5 and a PIN key 6. The IPIN key 5 is used when entering the collation number IPIN (Initialization Personal Identification Number) into the IC card 8 connected to a card insertion port 7 provided on a side of the main body. The PIN key 6 is used similarly when registering the password number PIN (Personal Identification Number). The above-mentioned collation number IPIN is a random, for example, 6-bit code for use until the password number PIN of the card owner is used. A changeover switch 9 is provided on the same side of the main body as that having the card insertion port provided thereon to select a kind of data entered from the IC card upon confirming the password information.

The circuit configuration of the printer-calculator having the above-mentioned terminal will now be described with reference to Fig. 2.

In Fig. 2, reference numeral 11 represents a bus line. A password information memory 12, an input control part 13 which controls the keyboard 2, an arithmetic control part

14, a system ROM 15, a system control part 16, a display control part 17 which controls the display part 3, and a print control part 18 which controls the printer (printing part) 4 are connected to this bus line 11. The IC card 8 is  
5 connected to the above-mentioned bus line 11 via a connecting terminal 20 from an interface part 19. When registering password information to the IC card 8 connected by the connecting terminal 20, from the keyboard 2 via the bus line 11 and the interface part 19, the password  
10 information memory 12 previously stores the password information in response to a memory position at which data intrinsic to the IC card is written in, simultaneously with this registration. In this example shown, pieces of password information corresponding to data X1, X2, .....  
15 intrinsic to a plurality of kinds of IC card are represented by PIN 1, PIN 2, ..... The card-intrinsic data X1, X2, ..... are read out from the IC card 8 and set upon PIN-setting registration of the IC card 8 by the terminal. The pieces of password information PIN 1, PIN 2,  
20 ..... intrinsic to the individual cards stored in the password memory are taken out upon receipt of an OK signal, described later, from the IC card connected, and outputted to the display part 3 via the display control part 17, or to the print part 4 via the print control part 18.

25 The circuit configuration of the IC card 8 will now be described with reference to Fig. 3.

In Fig. 3, reference numeral 21 represents a connecting

terminal opposite to the connecting terminal 20 of the printer-calculator 1. The connecting terminal 21 is connected to a bus line 23 via the interface part 22. A system ROM 24, a system control part 25, a passbook memory 26 and an IC card-specific data memory 27 are connected to this bus line 23. This IC card-specific data memory 27 stores, for example, 64-bit data X different from each other for identifying individual IC cards. When manufacturing cards, these card-intrinsic data X are written as data, for example, intrinsic to the card issuer company. Various data including paid-in, paid out and balance data are also written into the passbook memory 26. In addition, an IPIN memory 28, a PIN memory 29 and a password information retaining RAM 30 are connected to the bus line 23. A collation number (IPIN) written previously upon manufacturing the card is stored in the IPIN memory 28, and a password number (PIN) written from the keyboard 2 by the card owner himself/herself upon connecting the card 8 to the printer-calculator 1 with a terminal is stored in the PIN memory 29. On the other hand, a collation number IPIN entered from the keyboard 2 of the printer-calculator 1, or a password number PIN fetched from the password information memory 12 on the basis of certain conditions described later is supplied to the above-mentioned password information retaining RAM 30 via the interface parts 19 and 20, respectively, and temporarily retained there. A comparing part 31 is connected to the IPIN memory 28, the



PIN memory 29 and the password information retaining RAM 30. A comparison output signal from the comparing part 31 is supplied to the system control part 25. The comparing part 31 compares and collates the collation number (IPIN) or the password number (PIN) stored in the memories 28 and 29 with the collation number IPIN or the password number PIN temporarily stored and retained in the RAM 30 to determine whether or not there is consistency. When there is consistency, the system control part 25 send out an OK message to the printer-calculator 1. If not, a BAD message is sent out.

#### Operations when setting a password number PIN in the IC

card 8 with the above-mentioned device in this embodiment on the basis of the information of the IC card sent from the card issuer company to the card owner and information of the collation number IPIN sent by separate cover will now be described with reference to the flowcharts shown in Figs. 4 and 5.

Fig. 4 is a flowchart in the printer-calculator 1 with the terminal, and Fig. 5 illustrates a flowchart in the IC card 8. First in step A1, an end of the IC card 8 is inserted into the card insertion port 7 of the printer-calculator with terminal 1, to achieve electric connection between the connecting terminal 20 on the terminal side and the connecting terminal 21 on the card side. Then in step A2, a collation number IPIN sent from the card issuer

company separately from the IC card is entered from the keyboard 2. In step A3, this IPIN data is sent to the IC card 8 side via the interface part 19 and the connecting terminal 20. Then, on the IC card 8 side, in step B1, the  
5 collation number IPIN data sent from the terminal side is received, and temporarily stored and retained in the password information retaining RAM 30. Then in step B2, this collation number IPIN and the collation number (IPIN) previously stored in the IPIN memory 28 are compared and  
10 collated in the comparing part 31 to determine whether or not these numbers are consistent with each other. In this step B2, if the result is Y (Yes), i.e., if it is determined that these collation numbers are in agreement [IPIN = (IPIN)], the person holding this IC card 8 is determined to  
15 be the true card owner. Then in step B3, the system control part 25 on the card side transmits an OK message via the interface part 22. Then on the terminal side, the message signal from the card side is received on the terminal side in step A4, and in step A5, it is determined whether or not  
20 the received message signal is an OK signal. If the result in this step A5 is Y (Yes), the process advances to step A6, in which the card owner enters a password number PIN set arbitrarily by himself/herself by using the keyboard 2. Then in step A7, the password number PIN is transmitted to  
25 the card side, and in step A8, a specified data X read out from the IC card 8 and the password number PIN are stored in the password information memory 12. Along with this, the

card side receives, in step B4, the password number PIN entered on the terminal side, and in step B5, the received password number is stored in the PIN memory 29. As a result, it becomes possible to register the password number PIN into the IC card 8 without being noticed by any one other than the card owner, and it is made possible to use the card. Subsequently, by performing setting and registration of PINs in a plurality of IC cards of different kinds in a similar manner, data intrinsic to the individual cards x2, X3, ..... and password numbers PIN2, PIN3, ..... are sequentially written at memory positions corresponding to these card-intrinsic data every time in the password information memory of each terminal.

On the other hand, if step B2 results in N (No), i.e., if the collation number (IPIN) previously registered on the card side does not agree with the collation number IPIN entered from the terminal side, the process advances to step B6, and the system control part 25 on the card side transmits a BAD message to the terminal side. This results in determination of N (No) on the terminal side in step A5, thus permitting issuance of error determination. In this case, it is determined that there occurs an input error in step A2, or the IC card 8 itself does not correspond to this terminal, and it is necessary to conduct again operations from step A1 or A2.

The reading operation of PIN in a case where, during use

of an IC card 8 after setting a password number PIN as shown in Figs. 4 and 5, the card owner forgets his/her password number pin, will now be described with reference to the flowcharts shown in Figs. 6 and 7.

5            Fig. 6 is a flowchart in the printer-calculator 1 with a terminal, and Fig. 7 is a flowchart in the IC card 8. First in step C1, an end of the IC card 8 of which the password number PIN is forgotten is inserted into the card insertion port 7 of the printer-calculator 1 with a terminal to  
 10 achieve electric connection of the respective connecting terminals 20 and 21. As a result, in the IC card 8, as shown in step D1, a data X intrinsic to this card is fetched by the IC card-specific data memory 27 in accordance with a program stored in the system ROM 24, and transmitted as  
 15 data for specifying the card. Then, on the terminal side, as shown in step C2, the specified data from the card side is received, and the process advances to C3. In this step C3, intrinsic data X1 in the corresponding password information memory 12 is retrieved on the basis of the  
 20 specified data X from the card side, and the password number PIN stored at the memory position is recognized as corresponding to this IC card 8 and specified. Subsequently, the process goes to step C4, and the password number PIN1 specified in step C3 is fetched from the  
 25 password information memory 12 and transmitted to the IC card 8. As a result, on the card side, as shown in step D2, the password number PIN sent from the terminal side is

received, and temporarily stored and retained in the password information retaining RAM 30. Then in step D3, PIN retained in the RAM 30 after receiving is compared and collated with (PIN) set and registered in the PIN memory 29  
5 by the comparing part 31. If step D3 results in Y (Yes), i.e., if it is determined that these password numbers are in agreement [PIN = (PIN)], and this card 8 corresponds to the printer-calculator 1 with terminal currently in connection, the system control part 25 transmits an OK  
10 message in step D4. Then, the terminal side receives, in step C5, the message signal from the card side, and in step C6, determines whether or not this message signal is an OK message. If step C6 results in Y (Yes), i.e., if it is determined that the message signal from the card side is an  
15 OK signal, and the IC card 8 currently in connection is the one for which PIN is set and registered by the terminal 1, the process advances to step C7, in which the password number PIN1 specified in step C3 is fetched from the password information memory 12 through specification by the  
20 system control part 16, and is displayed on the display part 3 via the display control part 17. In this case, PIN1 of the IC card displayed by the display part 3 disappears after display for only a relatively short period of time (for example, 5 seconds). The card owner can therefore  
25 know PIN of his/her IC card 8 without being known by others at all, and use this card again as usual.

Subsequently, in step C8, the system control part 16

and the arithmetic control part 14 determine at which of 1, 2 and 3 switching positions the changeover switch 9 is set. If determination results in the switching position 1, the process goes to step C9. In this step C9, PIN data other than the password number PIN1 already displayed in step C7 (PIN2, PIN3, ....., in this case) are fetched from the card side as shown in step D5 and displayed on the display part 3. This permits immediate confirmation of any other card password number than the IC card 8, if forgotten by the card owner. When determination gives the switch position 2 in step C8, the process advances to step C10. The terminal 1 fetches balance data in the passbook memory 26 in the IC card 8 in the same manner as above in step D5 and displays the same on the display part 3. As a result, the card owner can confirm not only the forgotten PIN, but also the balance in the passbook. When determination in step C8 gives a result of switch position 3, various data in the card as those displayed in steps C9 and C10 are fetched in step D5 from the card side, and sequentially printed in the print part 4 via the print control part 18. As a result, it is also possible to confirm the above-mentioned passbook data by printing.

If step D3 on the card side gives a result N (No), i.e., if it is determined in step C4 that PIN sent from the terminal side is not consistent with (PIN) already set and registered in the card, and this IC card does not correspond to the printer-calculator 1 with terminal, the

process goes to step D6, and the system control part 24 on the card side transmits a BAD message to the terminal side. Then, in step C6 on the terminal 1 side, determination gives a result N (No), i.e., it is determined by the

5 terminal 1 that the IC card 8 is not one registering PIN, and the flowchart of password information confirmation is determined to be in error. In this case, the IC card 8 has highly probably been stolen somewhere, and the password information in the terminal or various data such as other  
10 passbook data are not displayed or printed at all in this state. As a result, the contents of the card are never known by a wrong owner of the card.

Therefore, even when the true card owner forgets his/her own password number PIN, it is possible to confirm  
15 his/her PIN again without the risk of being known by any other. In this case, for a stolen IC card, the card contents are never known unless the terminal corresponding to the card is stolen together, thus permitting prevention of fraudulent use.

20 The printer-calculator 1 with terminal in the above-mentioned embodiment may be managed by the card owner, may  
be managed in a lump by the card issuer company. In the case of management by the card issuer company, the card  
25 owner would visit the issuer company for above-mentioned setting or confirmation of PIN. In this case, the terminal 1 is installed at the counter of the card issuer company.

The terminal 1 in the above-mentioned embodiment is of course applicable as a printer-calculator as shown in Fig.

1.

#### 5 [Advantages]

According to the present invention, as described above, password information is written into the IC card and previously stored in the device to permit recognition of the kind of card by means of an intrinsic signal from the IC  
10 card connected later. The password information previously stored as described above corresponding to a recognized specific IC card is compared and collated with the password information stored by the specific IC card itself, and the password information is outputted and can thus be confirmed  
15 when these collated pieces of password information are in agreement. For example, when the card owner forgets his/her password number, therefore, it is possible to confirm again the password information stored in the card, and it is very difficult for a wrong user of the card to  
20 know the contents of the card. The present invention can thus provide such a confirming device for password information of an integrated circuit card.

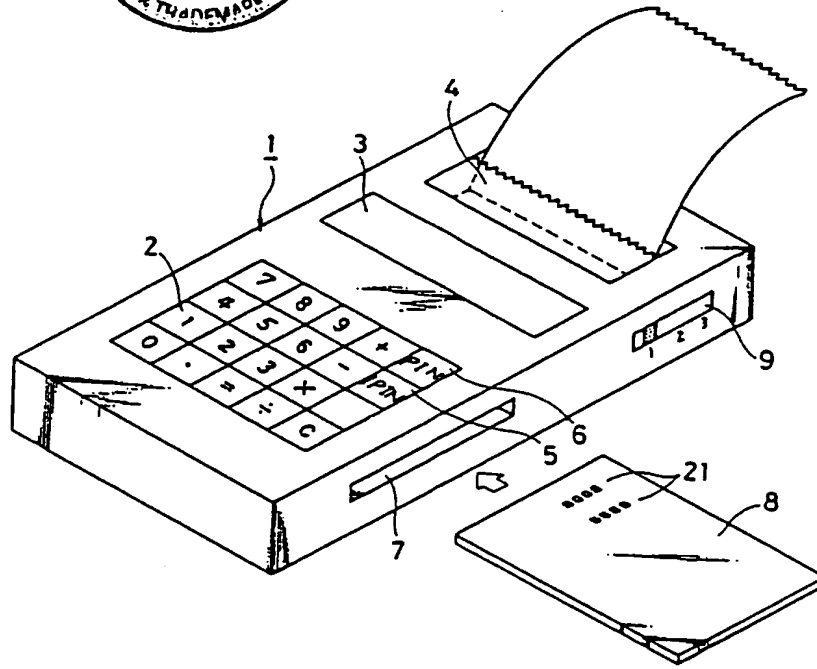
#### 4. Brief description of the Drawings

25 Fig. 1 is an exterior configuration view illustrating the IC card password confirming device of an embodiment of the present invention; Fig. 2 is a circuit configuration

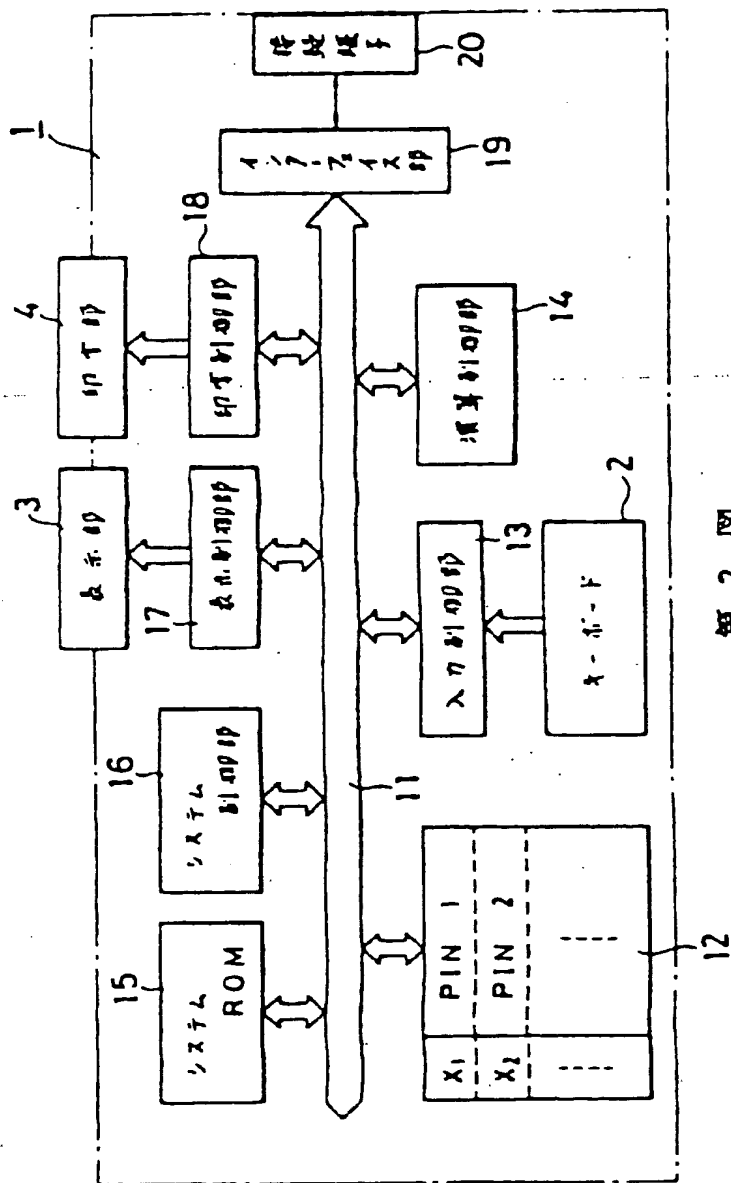


diagram of the printer-calculator with terminal in the IC  
 card password information confirming device shown in Fig.  
 1; Fig. 3 is a circuit configuration diagram illustrating  
 an IC card in the IC card password information confirming  
 5 device shown in Figs. 1 and 2; Figs. 4 and 5 are flowcharts  
 illustrating operations on the terminal side and the card  
 side upon setting a password number PIN by the IC card  
 password information confirming device, respectively; and  
 Figs. 6 and 7 are flowcharts illustrating operations on the  
 10 terminal side and the card side upon confirming the  
 password number PIN by the IC card password information  
 confirming device, respectively.

1: Printer-calculator with terminal, 2: Keyboard, 3:  
 Display part, 6: PIN key, 7: Card insertion port, 8: IC  
 15 card, 11, 23: Bus line, 12: Password information memory,  
 19, 22: Interface part, 20, 21: Connecting terminal, 27:  
 IC card specifying data memory, 29: PIN memory, 30:  
 Password information retaining RAM, 31: Comparing part.



第 1 图

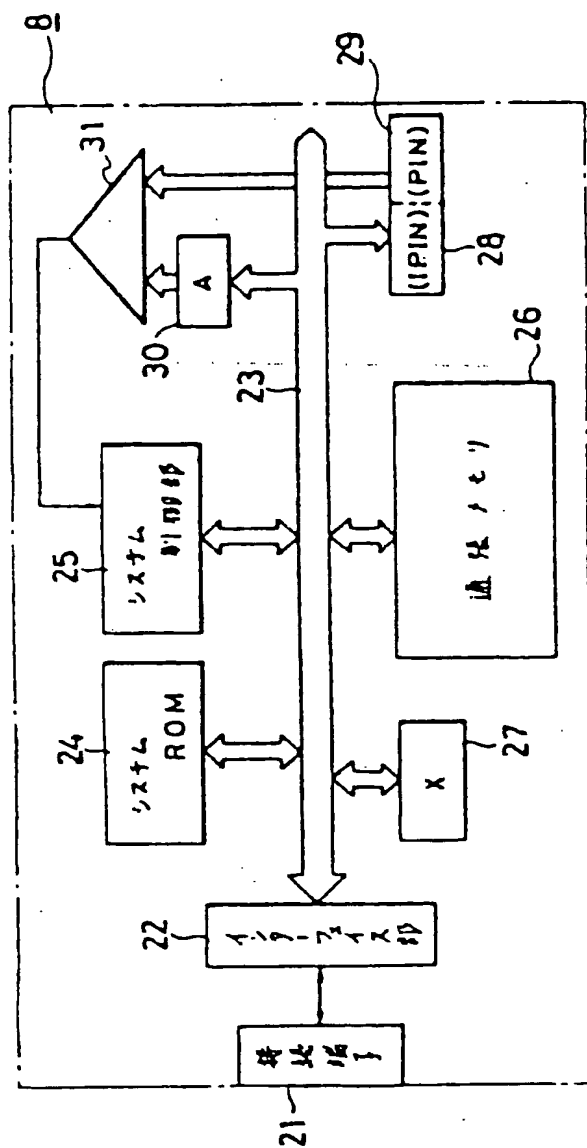


第 2 図



FIG. 2

- 2: KEYBOARD
- 3: DISPLAY PART
- 4: PRINT PART
- 5 13: INPUT CONTROL PART
- 14: ARITHMETIC CONTROL PART
- 15: SYSTEM ROM
- 16: SYSTEM CONTROL PART
- 17: DISPLAY CONTROL PART
- 10 18: PRINT CONTROL PART
- 19: INTERFACE PART
- 20: CONNECTING TERMINAL



第 3 図



FIG. 3

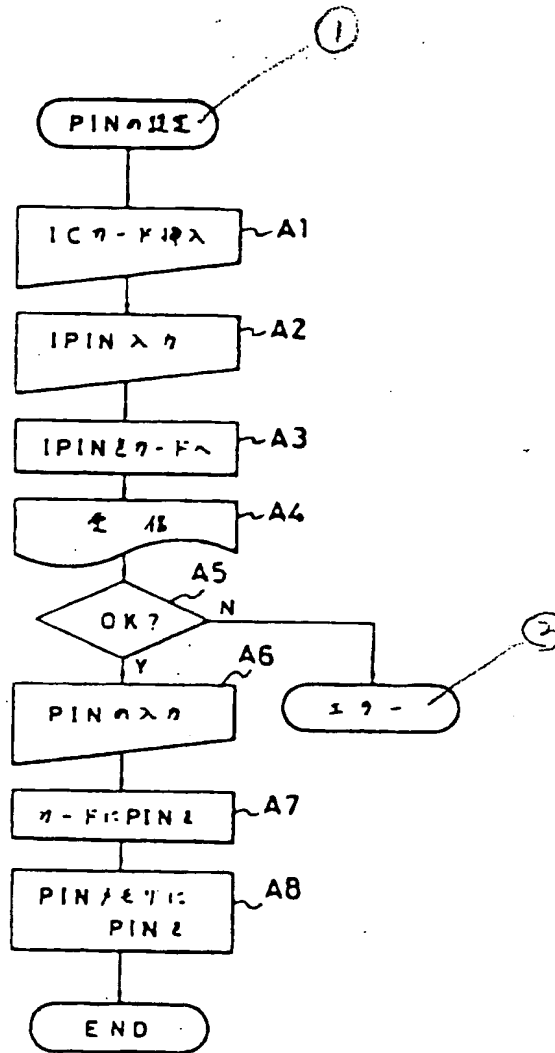
21: CONNECTING TERMINAL

22: INTERFACE PART

5 24: SYSTEM ROM

25: SYSTEM CONTROL PART

26: PASSBOOK MEMORY





RECEIVED

AUG 28 2003

Technology Center 2100

FIG. 4

(1) SET PIN

A1: INSERT IC CARD

5 A2: INPUT IPIN

A3: SET IPIN IN CARD

A4: RECEIVE

(2) ERROR

A6: INPUT PIN

10 A7: SET PIN1 IN CARD

A8: SET PIN2 IN PIN MEMORY